REMARKS

Reconsideration and allowance are respectfully requested in view of the following remarks.

Of pending claims 1-2, 4-17, 19-22, and 24-28, claims 1, 16, and 21 are independent.

Claim Rejections Under 35 U.S.C. § 103

Claims 1-2, 4-12, 14-17, 19-22 and 24-28 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Hanna et al. (WO-0172012, hereinafter "Hanna") in view of Connery et al. (U.S. Patent No. 6,606,709, hereinafter "Connery").

Claim 13 is rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Hanna in view of Silen et al. (U.S. Patent Application Publication No. 2002/0045442, hereinafter "Silen") and Bird (U.S. Patent 5,148,479).

These rejections are respectfully traversed, because none of the documents relied upon disclose or provide any reason whatsoever for dispatching a system communication such as a warning or alarm, by a communication device assigned to a system, such as a system for industrial electricity, water or heat, wherein the system communication comprises: (1) information relating to the system; (2) a validation code; and (3) validity information. The claimed communication device processes a message received after the communication has been dispatched, and verifies that the message (e.g., a control signal for responding to the warning or alarm) is received within the limited period of validity defined by the validity information. Thus, a time frame for responding to a warning or an alarm signal can be used as part of an authentication process for authenticating a message that

instructs corrective action of the system. None of the documents relied upon by the Examiner disclose, or provide any reason to include, such an authentication process, because none of these documents is directed to generating a message within a limited period of time that is defined by a system communication.

Embodiments of the Disclosure

Exemplary embodiments of the disclosure are directed to a method for remotely controlling and/or regulating at least one system, such as the system 1 of Applicants' Fig. 1. In an exemplary method, the validation code is generated that has a limited period of validity, and this validity code is appended to a system communication such as a system alarm signal. The validation code is valid only once for a communication to be dispatched. Validity information is added to the validation code to define a limited validity period for the validation code, within which a responsive message must be received.

In the Fig. 1 embodiment, a communication device 2 assigned to the system 1 dispatches a communication that includes the validity information, the information relating to the system, and the validation code .

In exemplary embodiments, the communication can be triggered by an error in the system 1, such as ambient temperature, which exceeds a limit. Thus, the communication can constitute an alarm, for example. See page 6, line 18-30.

A message is received and processed by the communication device 2 in response to the system communication, and is processed to extract a check code. The validation code and the check code are used to check (i.e., authenticate) whether the message originated from a receiver of the communication within a limited period of validity. If the checking and the verifying are successful, instruction

information is extracted from the message, and the system 1 can implement corrective action.

Independent claims 1, 16 and 21 broadly encompass the foregoing features.

Independent claim 1 recites a method including adding validity information to a validation code, which validity information defines the limited period of validity of the validation code. The claim 1 method includes dispatching the communication by a communication device assigned to the system, where the communication comprises (a) the information relating to the system, (b) the validation code, and (c) the validation information. Claim 1 recites processing a message which the communication device receives after the communication has been dispatched, where the processing includes (a) extracting a check code from the message according to a first extraction rule (b) checking whether the message originates from a receiver of the communication based on the validation code and the check code, and (c) verifying whether the message is received within the limited period of validity defined by the validity information.

The Connery Document

Connery is directed to a system wake-up, and is not responsive to a system communication. In the Connery patent, a system (Fig. 1) for remote management and wakeup utilizes "magic packet" sent in one direction from a network management station 21 to a NIC (network interface cards 13, 14, 15) of an end system (10, 11, 12). As shown in Figs. 4 and 5 of Connery, the magic packet can include a timestamp 84, random value token 85, and message authentication code 86. The timestamp 84 and random value token 85 of Connery are both generated at the network management station 21 so that they can be included in the magic

packet. See col. 7, lines 35-43 of Connery. The message authentication code 86 is based on a secret shared between the end system NIC and the network management station 21. See col. 8, lines 2-15 of Connery. In Connery's system, the secret is the same for every packet sent.

In contrast to exemplary embodiments of the disclosure, Connery requires a synchronization of the NIC timer with the timer of the network management system 21. See col. 8, lines 25-40. This synchronization facilitates the independent generation of time values and random numbers by the NIC and the network management system 21. The magic packet is received by the end system NIC, where the timestamp 84, random value token 85, and message authentication code 86 are tested for validity. There is, however, no responsive message received and processed by a communication device within a limited period of validity that is defined by a system communication as presently claimed by Applicants.

The Hanna Document

Hanna discloses a method for providing security between a device controller 12 and a device 11 by establishing a shared secret, in the form of an authentication value. See page 7, first full paragraph of Hanna. The Examiner apparently considers the shared secret of Hanna to be analogous to the shared secret of Connery.

However, the Examiner acknowledges that the authentication value of Hanna is (1) not valid only once, (2) not valid for a limited period, and (3) not accompanied by a validation information defining the limited period (final Office Action, page 3). There is no responsive message received and processed by a communication device within a limited period of validity that is defined by a system communication as presently claimed by Applicants.

The Examiner Has Failed To Establish a Prima Facie Case Of Obviousness Based On The Hanna and Connery Combination

Because the Hanna and Connery documents fail to disclose or provide any reason to provide a responsive message received and processed by a communication device within a limited period of validity that is defined by a system communication as presently claimed by Applicants, Applicants' claim 1 is allowable.

Connery sends the magic packet, which contains timestamp 84, random value token 85, and message authentication code 86, from a network management station 21 to an end station NIC. The use of nonces and timestamps in Connery requires synchronization of the clocks of the network management station 21 and the NIC.

In exemplary embodiments of the claimed invention, a communications device connected to a system can send a communication to a receiver, the communication including validity information defining a limited period of validity and a valid-once validation code. The applied Connery document, however, sends a magic packet in an opposite direction: from a receiver to a communications device connected to a system, assuming, *arguendo*, that the network management station 21, NIC, and end station of Connery can be considered to respectively correspond to a receiver, communications device, and system, which Applicants do not concede. Thus, the magic packet cannot correspond to the message or the communication as recited in claim 1.

The Examiner states that "one time random numbers or nonce having a period of validity to protect messages transferred between two systems is well known in the art". Even if, *arguendo*, this were true, such a configuration would not include a communication dispatched by a communication device to a receiver, and

an instruction-containing message sent by the receiver to the communication device within a limited period of validity established by the communication.

Moreover, the shared secret of Connery cannot correspond to the communication of Applicants' claim 1 because, like the shared secret authentication code of Hanna, the shared secret of Connery is (1) not valid only once, (2) not valid for a limited period, and (3) not accompanied by a validation information defining the limited period.

Combined, the teachings of the Connery and Hanna documents would not have resulted in the features of Applicants' claim 1 because neither of these documents disclose or provide any reason to include features recited in Applicants' claim 1. As such, claim 1 is allowable.

Independent claims 16 and 21 are allowable for at least similar reasons to those provided above with respect to claim 1.

The Silen and Bird documents do not cure the deficiencies of Hanna and Connery.

Accordingly, Applicants' claims 1, 16 and 21, and all claims depending therefrom, are allowable.

Conclusion

From the foregoing, further and favorable action in the form of a Notice of Allowance is respectfully requested.

In the event that there are any questions concerning this amendment, or the application in general, the Examiner is respectfully requested to telephone the undersigned so that prosecution of present application may be expedited.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: November 22, 2010

By: Michael Keeney #63985
for Patrick C. Keane
Registration No. 32858

Customer No. 21839
703 836 6620